MODUS OPERANDI TINDAK PIDANA *CRACKER* MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Nur Khalimatus Sa'diyah
Fakultas Hukum Universitas Wijaya Kusuma Surabaya
e-mail: nurkhalimatus@yahoo.com

ABSTRAK

Penulisan hukum ini dilatarbelakangi bahwa teknologi informasi memegang peranan penting dalam kehidupan manusia baik di masa kini maupun masa yang akan datang. Implikasi dari pertumbuhan teknologi informasi membawa masyarakat kepada pola perilaku yang semakin terbuka. Dengan kehadiran internet, maka membuat kehidupan manusia di seluruh dunia menjadi lebih mudah. Karena internet dapat menembus batas-batas antarnegara dan mempercepat penyebaran dan pertukaran ilmu baik di kalangan ilmuwan atau cendekiawan di seluruh dunia. Hanya saja, dibalik kemudahan penggunaan internet, terdapat sisi gelap yang merisaukan penggunanya, yaitu dari segi keamanannya. Keamanan sistem komputer berbasis internet perlu diperhatikan. Karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan dunia maya atau *cyber crime*. Terutama kejahatan *cracker*. *Cracker* adalah pelaku atau orang yang melakukan aktivitas *cracking* di internet. Akibat dari kejahatan tersebut sangat merugikan. Diantaranya adalah dapat merusak jaringan, situs tidak dapat dibuka, terhapusnya data-data dan lain-lain. Karena modus operandi *cracker* ini berbeda dengan kejahatan konvensional lainnya. Dan yang paling membedakan adalah *locus delicti*nya atau tempat kejahatan perkara. Setelah mengetahui modus operandi *cracker*, maka akan dengan mudah untuk dapat menangani kasus *cracker*.
Kata Kunci: modus operandi, *cracker*, Undang-Undang Informasi dan Transaksi Elektronik.

ABSTRACT

This legal research based on the fact that information technology plays an important role in human being nowadays and also in the future. The implication of the massive information technology development brings different behavior to some people. By the presence of the internet, it makes human being life become easier. Internet could definetely access data over countries, and could also be useful in knowledge exchange among scientists or scholars around the world. However, eventhough internet is ease of use, there are some risk which could harm the user, especially from the safety aspect. Thats why the safety of the internet based computer system security must be considered. Because the character of internet network is global public open access, it makes internet network become very vulnerable from any cyber crimes, especially cracking crime. Cracking is the activity while cracker is the person who done the cracking activity over the internet network. The effects of this crime are very harmful, such as broken network, broken website, and even worse, data loss. Because the cracker's modus operandi is definetely different from other conventional crime, and the most prominent difference is the locus delicti (place where the crime happened), because tracking the internet network is not easy. Therefore by knowing the cracker's modus operandi, it will be easier to resolve the cracking cases.
Keywords: *modus operandi, cracker, cracking, ITE Law.*

PENDAHULUAN

Teknologi informasi memegang peranan penting, baik di masa kini maupun di masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang sangat besar bagi negara di dunia. Adapun implikasi dari pertumbuhan teknologi informasi membawa masyarakat kepada pola perilaku yang semakin terbuka. Masyarakat tidak lagi hanya menerima akses informasi dari media massa yang

perlu menunggu waktu sehari atau satu jam. Dengan kehadiran teknologi ini, informasi yang diinginkan bisa didapatkan dalam hitungan menit atau detik, yakni melalui media internet.

Perkembangan internet yang pada awal mulanya hanya digunakan untuk kepentingan kekuasaan dan internet dikembangkan pada tahun 1960 oleh Amerika Serikat khususnya untuk kepentingan militer. Pada tahun 1970-an kalangan akademisi mulai menggunakan internet sebagai jaringan komputer yang dapat menghubungkan lembaga-lembaga akademis dalam universitas (Gareth Grainger, 2000:72-73). Namun dalam perjalanannya, internet saat ini sudah dapat dinikmati oleh semua kalangan, baik kalangan *elite* maupun biasa.

Internet saat ini dapat diakses melalui *software* seperti *Netscape, Mosaic, The Internet Explorer,* dan penyedia lainnya melalui jasa komersial seperti *America Online* dan *Prodigi*. Melalui penggunaan s*oftware* seperti di atas, maka pemilik komputer dapat memasukkan dokumen kedalam komputernya, dan sekaligus pula si pemilik komputer dapat mengakses dan membaca dokumen. Selain itu pengguna internet dapat melakukan perjalanan untuk mencari dokumen-dokumen yang ditempatkan dengan jumlah ribuan. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan *Cyberspace*.

Hanya saja, dibalik kemudahan dan kenyamanan penggunaan internet itu ternyata tidak selamanya demikian karena dalam *cyberspace* juga terdapat sisi gelap yang perlu kita perhatikan. Disana ada ancaman yang sangat merisaukan, yakni sisi keamanannya. Pengamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan. Ancaman timbul manakala seseorang mempunyai keinginan memperoleh akses ilegal ke dalam jaringan komputer, merusak jaringan, mengubah suatu tampilan dengan tampilan lain yang merugikan banyak pihak. Kemudian lahirlah perilaku-perilaku yang menyimpang dengan memanfaatkan teknologi canggih sebagai alat untuk mencapai tujuan, dengan cara melakukan kejahatan. Kejahatan-kejahatan ini, dikenal sebagai kejahatan dunia maya atau yang biasanya disebut dengan *cybercrime.*

Cybercrime menggunakan media komunikasi yaitu internet dan komputer, kendati berada di dunia lain dalam bentuk maya tetapi memiliki dampak yang sangat nyata. Penyimpangan dan kerugian besar telah terjadi dan dirasakan oleh masyarakat di berbagai penjuru dunia. Bahkan kerugian berdampak luas pada sektor-sektor lain di bidang ekonomi, perbankan, moneter dan sektor lain yang menggunakan jaringan komputer.

Bilamana seseorang akan menggunakan atau yang memakai komputer, atau bagian dari suatu jaringan komputer tanpa seijin yang berhak, maka tindakan tersebut sudah tergolong pada kejahatan komputer. Keragaman aktivitas kejahatan internet yang berkaitan dengan komputer atau jaringan komputer sangatlah besar dan telah menimbulkan perbendaharaan bahasa baru, misalnya *hacking, cracking, virus, time bomb, worm, trojan horse, logical bomb, spaming, hoax*, dan lain-lain sebagainya. Masing-masing memiliki karakter berbeda dan implikasi yang diakibatkan oleh tindakannya pun tidak sama. Kecemasan terhadap *cybercrime* ini telah menjadi perhatian dunia, namun tidak semua negara di dunia ini memberikan perhatian yang lebih besar terhadap masalah *cybercrime* dan memiliki peraturannya (kecuali negara-negara maju dan beberapa negara berkembang).

Indonesia sebagai negara berkembang memang sangat terlambat dalam mengikuti perkembangan teknologi informasi. Hal ini tidak lepas dari strategi pengembangan teknologi yang tidak tepat karena mengabaikan riset sains dan teknologi. Akibatnya, transfer teknologi dari negara industri maju tidak diikuti dengan adanya penguasaan terhadap hal itu sendiri yang mengantarkan Indonesia kepada negara yang tidak mempunyai basis teknologi. Keterlambatan ini dapat membawa dampak jika terjadi kejahatan *cybercrime* maka perangkat hukum yang mengatur mengenai *cybercrime* tidak ada dan penegak hukum merasa kesulitan karena tidak ada pedoman dalam menindak para pelaku perbuatan tersebut. Selain karena adanya faktor kesadaran hukum masyarakat Indonesia dalam merespon aktifitas *cybercrime* masih kurang, juga dikarenakan kurangnya pemahaman dan pengetahuan masyarakat tentang jenis kejahatan *cybercrime.* Dan juga karena faktor keamanan pelaku dalam melakukan tindak pidana, dimana internet menyediakan fasilitas untuk menghapus data atau *file* yang ada sehingga para pelaku dapat dengan mudah menghapus semua jejak kejahatan yang telah dilakukannya.

Kenyataan ini menjadi persoalan yang seringkali sulit dipecahkan, karena di samping perbuatan melawan hukum itu dilakukan oleh subyek yang menggunakan sarana teknologi canggih dan sulit dilacak keberadaannya sehingga menyebabkan pembuktiannya menjadi lebih sulit dibandingkan dengan perbuatan melawan hukum biasa meskipun pelakunya tertangkap. Namun perbuatan melawan hukum di dunia *cyber* juga sangat tidak mudah diatasi hanya

dengan mengandalkan hukum positif konvensional Indonesia (M. Ahmad Ramli, 2004:5).

Dari sekian banyak sisi gelap yang ada dalam *cybercrime*, yang paling banyak mendapat perhatian adalah perbuatan kejahatan yang sering dilakukan oleh *cracker*. Fenomena *cracker* dalam tahun-tahun terakhir ini memang mencemaskan karena mereka telah menggunakan keahliannya untuk melakukan kejahatan. *Cracker* dengan aktivitas *cracking*-nya mempunyai sejarah yang panjang, tetapi berdasarkan catatan, *cracking* yang dilakukan *cracker* pertama kali dilakukan pada tanggal 12 Juni terhadap *The Spot* dan tanggal 12 Agustus 1995 terhadap *Cracker Movie Page.* Berdasarkan catatan itu pula, situs dari pemerintah Indonesia pertama kali mengalami suatu serangan *cracker* pada tahun 1997 sebanyak 5 (lima) kali, yaitu tanggal 19 Januari, 10 Februari, 24 April, 30 Juni dan 30 November. Pada tahun yang sama situs *NASA* (5 Maret), *UK Conservative Party* (27 April) dan *Spice Girls* (14 November) juga diserang oleh *cracker* (Agus Raharjo, 2002:35).

Sejak serangan yang pertama itu sampai sekarang, korban-korban serangan *cracker* terus berjatuhan dan jumlahnya kian meningkat pesat. Akan tetapi, hampir sebagian besar tidak terpublikasi sehingga data yang akurat mengenai berapa jumlah yang telah menderita akibat serangan *cracker* tidak dapat dicatat dan dihitung secara pasti. Indonesia meskipun dapat dikatakan tertinggal dalam mengikuti dan menikmati perkembangan teknologi informasi, juga telah menjadi korban *cracking*

Bahkan, sistem *online* yang diterapkan dalam Penerimaan Siswa Baru (PSB) tahun ini ternyata masih menjadi sasaran para *cracker.* Penerimaan Siswa Baru yang *online* melalui jaringan internet mendapatkan serangan dari *cracker* sebanyak dua kali dengan penyerang yang berbeda sehingga menyebabkan para pengakses yang ingin masuk ke dalam situs tersebut kesulitan (http:/continuousimprovement.blogsome.com/2006/07/24). Karena situs tersebut tidak dapat diakses dan dibuka. Untungnya data-data yang berada di dalam situs tersebut tidak sempat terhapus oleh para penyerang, dan masalah penyerangan tersebut dapat segera terdeteksi siapa pelakunya dan dapat dengan mudah di atasi sehingga tidak sampai menimbulkan kerugian yang cukup berarti.

Untuk mempermudah menangani kasus-kasus yang disebut *cracker* ini, maka pemerintah harus mengetahui dan memahami modus operandinya terlebih dahulu. Karena modus operandi *cracker* ini berbeda dari tindak kejahatan konvensional lainnya. Yang paling mencolok, perbedaan tersebut antara lain adalah *locus delicti* atau tempat kejahatan perkara, karena sangat sulitnya melokalisir jaringan internet. Bagaimana modus operandi *cracker* dalam Pasal 30 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang selanjutnya disebut UU ITE).

PEMBAHASAN

Terbentuknya Jaringan Komputer di Tengah Masyarakat

Modus operandi *cracker* ini berbeda dengan tindak kejahatan konvensional. Hal yang paling mencolok dari perbedaan tersebut antara lain adalah terletak pada *locus delicti* atau tempat kejahatan perkara, karena dalam kejahatan ini yang diserang adalah jaringan komputer atau internet. Sehingga dikatakan sulit karena memang sulitnya melokalisir jaringan internet, hal ini terkait dengan jaringan-jaringan yang ada pada komputer.

Pada tahun 1977, ada dua orang anak muda kreatif, Steve Jobs dan Steve Wozniak dari Lembah Silicon Valley, California. Mereka memperkenalkan konsep baru, sebuah *personal computer*, yang diberi nama *Apple* Komputer Generasi I. Dengan harapan satu orang satu komputer, ternyata konsep ini disambut hangat rakyat Amerika. Oleh karena itu kemudian komputer tersebut diberi nama *personal computer* (PC) atau komputer rumah tangga atau komputer pribadi. Ternyata prinsip-prinsip ini diadopsi oleh perusahaan-perusahaan lain. Perusahaan IBM dan Hawlett Packard yang dulunya bergerak di bidang komputer mini dan *mainframe* ikut terjun menambah ramai bisnis *personal computer* atau PC hingga seperti yang terjadi saat ini.

Dalam perkembangannya kehadiran dari *personal computer* atau PC berkembang dengan sangat pesat. Industri perangkat keras atau *hardware* komputer "membludak" dan menyebabkan harganya semakin murah, sehingga masyarakat umum semakin banyak yang mampu memiliki komputer di masing-masing rumah. Komputer pun pada akhirnya bukan lagi dapat di monopoli orang-orang kaya atau perusahaan besar atau kantor-kantor pemerintah, tetapi sudah terjangkau oleh sebuah rumah tangga yang sederhana. Bahkan, memiliki sebuah *laptop* atau *notebook* seolah-olah sudah menjadi hal yang biasa. Banyak yang bisa kita lihat di tempat-tempat umum adanya orang-orang yang tengah asyik dengan *laptop*nya. Orang yang menggunakan *laptop* tidak hanya bisa dilihat di kampus-kampus. Di bandara, rumah sakit, terminal, stasiun, pasar, *mall* dan sebagainya juga sudah terbiasa dijumpai orang-orang yang menggunakan *laptop*.

Kemudian terbentuklah sebuah jaringan komputer yang dapat tersambung antara yang satu dengan yang lain dalam posisi yang sama kuat. Jaringan internet itu menimbulkan kenyamanan bagi para operator komputer, karena memudahkan cara kerja pemakai komputer. Jaringan komputer yang saling terhubung melalui satelit ini kemudian dikenal dengan jaringan internet. Dengan adanya sistem jaringan internet pengakses dapat saling tukar pengetahuan, saling tukar informasi atau saling tukar data-data, antara komputer yang satu dengan komputer yang lain, dapat dilakukan dengan kecepatan yang cukup tinggi, tidak membutuhkan tempat yang besar, cukup dilakukan dari ruangan kecil yang menghemat biaya.

Dalam perkembangan, sebuah jaringan komputer atau jaringan internet merupakan suatu kebutuhan setiap orang, tiap perusahaan, dan setiap pemerintah. Pekerjaan yang biasanya dapat dilakukan berhari-hari bahkan berminggu-minggu, dengan hadirnya komputer jaringan atau internet biaya dapat dipangkas sedemikian rupa. Perasaan nyaman karena semua orang dapat bekerja lebih efektif dan efisien dengan sarana komputer dan internet. Hanya saja dalam perkembangannya kemudian jaringan itu digunakan sebagai sarana yang negatif, atau metode itu dapat dimanfaatkan oleh penjahat komputer untuk melihat, mengubah, atau merusak jaringan milik orang lain, seperti yang dilakukan oleh para *cracker*.

Kejahatan yang dilakukan oleh *cracker* adalah produk manusia modern, yang tidak memerlukan kekerasan fisik, namun dapat dikendalikan melalui suatu ruangan tertentu. Modalnya juga tidak terlalu besar, namun dapat menghasilkan uang yang cukup banyak dari hasil kejahatan tersebut.

Di Indonesia, kejahatan yang menggunakan sarana komputer sebenarnya sudah lama terjadi, namun pada saat ini sangat sulit di deteksi karena berbagai hal, baik lihat dari sumber daya manusianya, maupun dari sisi hukum yang memayunginya. Dari tahun ke tahun usaha untuk melakukan kejahatan ini terus meningkat, seiring dengan kemajuan teknologi dan kemajuan berfikir manusia. Di sisi lain, usaha-usaha untuk melakukan penegakan hukum masih belum ada perkembangannya.

Akibat kejahatan yang dilakukan *cracker* ini, nama Indonesia menjadi kurang baik karena masuk dalam daftar hitam di kalangan penyedia layanan-layanan pembayaran lewat internet atau *online payment*. Hal ini sungguh memprihatinkan karena pada masa yang sulit ini akibat krisis ekonomi, Indonesia sebenarnya tengah memulihkan namanya di forum perdagangan internasional. Ketika sudah mulai diperhitungkan dalam iklim investasi dunia karena berkat berbagai kemudahan dalam infrastruktur perdagangan global pembayaran atau transaksi melalui layanan internet, ternyata banyak tangan-tangan jahil yang berlaku tidak baik dengan melakukan kejahatan menggunakan internet sebagai sarananya.

Baik buruknya *output* atau hasil akhir dari suatu pemanfaatan komputer tergantung operatornya. Peran operator sangat menentukan apakah operasi yang dilakukan oleh operator merugikan banyak orang atau tidak, menyangkut perbuatan pidana atau tidak. Untuk memperjelas hal tersebut dikemukakan pendapat para ahli sebagai berikut. Suatu perbuatan bisa dijadikan perbuatan pidana atau dikriminalisasikan menurut TB. Ronny R. Nitibaskoro, karena alasan: Perbuatan itu merugikan masyarakat; Sudah berulang-ulang dilakukan; Ada reaksi sosial atas perbuatan itu; Ada unsur bukti.

Berdasarkan keempat parameter ini, maka tidak serta merta setiap perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana. Oleh karena itu, di dalam dunia *cyber* perlu dipilah dengan seksama, mana saja perbuatan-perbuatan yang layak dikategorikan sebagai kejahatan pidana seperti *cracker*.

Kejahatan yang dilakukan oleh *cracker* ini pada awalnya sulit dilacak, karena selalu ada suatu metode untuk menghilangkan jejak dengan logika yang sudah dikuasai oleh operatornya. Ada beberapa hal yang menyebabkan suatu kejahatan ini sulit dilacak antara lain: Di dalam sebuah perusahaan, data-data komputer biasanya ditangani oleh *Electronic Data Processing* (EDP), dimana disitu ada auditor; Masih sedikitnya pegawai-pegawai selaku operator komputer yang mengetahui cara kerja komputer secara rinci; Para pelaku kejahatan komputer adalah orang-orang yang pada umumnya cerdas dan mempunyai perasaan keingintahuan yang besar, fanatik akan teknologi komputer; Buku-buku tentang kejahatan komputer tidak banyak; Kejahatan komputer itu terselubung dan terorganisir. Tidaklah mudah bagi seseorang untuk menyelidiki kegiatan kejahatan komputer; Mudah dilakukan, resiko untuk ketahuan kecil dan tidak diperlukan peralatan yang super modern; Jarang sekali ada seminar-seminar atau mata kuliah tentang pencegahan terhadap kejahatan komputer; Terlalu percaya pada komputer; Kurangnya perhatian dari masyarakat.

Atas dasar hal-hal tersebut, lahirlah kesulitan para penegak hukum untuk menemukan kejahatan yang menggunakan sarana komputer seperti yang dilakukan oleh *cracker* atas aktivitas *cracking*nya di

internet. Disamping sulitnya melakukan pelacakan karena faktor di atas, juga karena faktor sumber daya manusianya. Untuk melakukan penyidikan terhadap kejahatan *cracker* ini harus mempunyai keahlian di bidang komputer dan jaringannya dan setelah itu perlu peranan ahli komputer yang secara teknis menerangkan kepada penyidik.

Modus Operandi *Cracker*

Adapun modus operandi yang dilakukan oleh para *cracker* dalam Pasal 30 UU ITE biasanya disebut *Unauthorized Access to Computer System and Service* yaitu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik resmi sistem jaringan komputer yang dimasukinya. Biasanya seorang pelaku kejahatan atau *cracker* melakukannya dengan maksud sabotase ataupun melakukan pencurian informasi penting dan rahasia.

Adapun Langkah-langkah yang dilakukan oleh *cracker* kurang lebih sama, sedangkan yang berbeda adalah dampak yang ditimbulkan. Suatu *cracking* bisa terjadi jika ada suatu akses ke dalam suatu sistem yang dituju atau dimasuki mengalami kerusakan, dan kerusakan tersebut bisa membuat sistem tidak berfungsi, dan harus dilakukan pembenahan secara besar-besaran terhadap suatu sistem komputer yang telah rusak. Adapun proses penyusupan dalam dunia *cracker* dibedakan menjadi beberapa tahapan yaitu sebagai berikut:

Pertama, *Footprinting* dan/atau Pencarian Data: *Cracker* baru mencari sistem yang dapat disusupi. *Footprinting* adalah merupakan kegiatan pencarian data berupa: Menentukan ruang lingkup atau *scope* aktivitas atau serangan; *Network enumeratin* atau menyeleksi jaringan; Interogasi jaringan; Mengintai jaringan. Semua kegiatan ini dapat dilakukan dengan alat atau *tools* dan merupakan informasi yang tersedia bebas di internet. Kegiatan *footprinting* ini dapat diibaratkan mencari informasi yang tersedia umum melalui buku telepon.

Kedua, yaitu *Scanning* atau Pemilihan Sasaran: Lebih bersifat aktif terhadap sistem sasaran. Disini diibaratkan *cracker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan *scanning* dengan demikian dari segi jaringan sangat *berisik* dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali dengan menggunakan *stealth scanning*. *Scanning tool* yang paling legendaris adalah *nmap* (yang kini tersedia pula untuk *Windows 9x/ME* maupun *DOS*), selain *SuperScan* dan *Ultrascan* yang juga digunakan pada sistem *Windows*. Untuk melindungi diri dari kegiatan scanning adalah memasang *Firewall* misalnya *Zone Alarm,* atau bila ada keseluruhan network, dengan menggunakan aplikasi *Intrusion Detection System* (IDS) misalnya *Snort.*

Ketiga, Enumerasi atau Pencarian Data Mengenai Sasaran: Sudah bersifat sangat *intrusif* (mengganggu) terhadap suatu sistem. Disini para penyusup dapat mencari *account name* yang absah, *password,* serta *share resources* yang ada. Pada tahap ini, khusus untuk sistem *Windows*, terdapat *port* 139 (*NetBIOS session service*) yang terbuka untuk *resource sharing* antar-pemakai dalam jaringan. beberapa orang mungkin berpikir bahwa *harddisk* yang di-*share* itu hanya dapat dilihat oleh pemakai dalam *LAN* saja. Kenyataannya tidak demikian. *NetBIOS session service* dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia. *Tools* seperti *legion*, *SMB Scanner,* atau *Shares Finder* membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka *resource share* tanpa pemberian *password*).

Keempat, Gaining Access atau dikatakan Akses Ilegal telah Ditetapkan: adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai *user* biasa. Ini adalah kelanjutan dari kegiatan *enumerasi*, sehingga biasanya disini seorang penyerang sudah mempunyai paling tidak *user account* yang absah, dan tinggal mencari *password*nya aja. Bila *resource share*-nya diproteksi dengan suatu *password*, maka *password* ini dapat saja ditebak (karena banyak yang menggunakan *password* sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui *dictionary attack* (mencobakan kata-kata dari kamus sebagai suatu *password*) atau *brute-force attack* (mencobakan kombinasi semua karakter sebagai *password*). Dari sini penyerang mungkin akan berhasil memperoleh *log-on* sebagai *user* yang absah.

Kelima, Escalating Privilege (Menaikkan atau Mengamankan suatu Posisi): Mengasumsikan bahwa penyerang sudah mendapatkan *log-on access* pada sistem sebagai *user* biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem *windows*) atau menjadi *root* (pada sistem *Unix* atau *Linux*). Teknik yang digunakan sudah tidak lagi *dictionary attack* atau *brute-force attack* yang memakan waktu itu, melainkan mencuri *password file* yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem *Windows 9x/ME password* disimpan dalam *file PWL* sedangkan pada *Windows NT/2000* dalam *file.SAM*. Bahaya pada tahap ini bukan hanya dari penyerang di luar sistem melainkan lebih besar

lagi bahayanya adalah orang dalam, yaitu *user* absah dalam jaringan itu sendiri yang berusaha naik kelas menjadi *admin* atau *root.*

Keenam, Pilfering atau Suatu Proses Pencurian: Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke *trusted system*. Mencakup evaluasi *trust* dan pencarian *cleartext password* di *registry, config file*, dan *user data*.

Ketujuh, Covering Tracks atau Menutup Jejak: Begitu kontrol penuh terhadap sistem yang diperoleh, maka menutup jejak menjadi suatu prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti macam-macam *rootkit* dan *file streaming*.

Kedelapan, Creating Backdoors atau Membuat Jalan Pintas: Pintu belakang diciptakan pada berbagai bagian dari suatu sistem untuk memudahkan masuk kembali. Pada tahap keenam, ketujuh dan kedelapan, penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan atau *pilfering*, menutupi jejak penyusupannya atau *covering tracks*, dan menyiapkan pintu belakang atau *creating backdoor* agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya *trojan* pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

Kesembilan, Denial of Service atau Melumpuhkan Sistem: Bukanlah tahapan terakhir, melainkan kalau penyerang sudah frustasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu *crash* atau kacau. *Denial of service attack* sangat sulit dicegah, sebab memakan habis *bandwidth* yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para *script kiddies* yang pengetahuan *cracking*-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

Beberapa modus dari kriminalitas yang dilakukan *cracker* di dunia maya, salah satu bentuknya yang wajib diwaspadai adalah pencurian data-data *account* penting. Pelaku biasanya adalah seorang *cracker* dengan cara menjebak orang lain untuk tidak sadar bersedia memberikan data-data *account*-nya. Modus yang digunakan adalah mengirimkan sebuah *e-mail phising* yaitu pengiriman *e-mail* yang bertujuan untuk mencuri data-data rahasia tentang *account*, *e-mail* seperti ini harus diwaspadai, caranya adalah dengan tidak mengindahkan dan menuruti perintah-perintah si *cracker* tersebut. Selanjutnya lakukan blokir alamat *e-mail* dari seorang pengirim *e-mail phising* tersebut. Adapun ciri-ciri umum dari *e-mail phising* adalah dengan memperhatikan dari *subject* dan *content*-nya, yaitu sebagai berikut: *Pertama, Verify your Account*. Kalau *verify*nya meminta *username, password* dan data lainnya, jangan memberikan reaksi balik. Maka harus selalu ingat *password* jangan pernah diberikan kepada siapa pun. Namun kalau ingin mendaftarkan *account* di suatu situs dan harus memverifikasinya dengan mengklik suatu *URL* tertentu tanpa minta mengirimkan data macam-macam, ya lakukan saja, karena ini mekanisme umum.

Kedua, If you don't respond within 48 hours, your account will be closed atau jika tidak merespon dalam waktu 48 jam, maka akun akan ditutup. Harap membaca baik-baik dan tidak perlu terburu-buru. Tulisan di atas wajib diwaspadai karena umumnya hanya propaganda agar pembaca semakin panik.

Ketiga, Dear Valued Customer. Karena *e-mail phising* biasanya targetnya menggunakan *random,* maka *e-mail* tersebut bisa menggunakan kata-kata ini. Tapi suatu saat mungkin akan menggunakan nama kita langsung, jadi harus waspada. Umumnya kebocoran nama karena kita aktif di *milis* atau forum komunitas tertentu.

Keempat, Click the link below to gain access to your account. Metode lain yang digunakan *cracker* yaitu dengan menampilkan sebuah *URL Address* atau alamat yang palsu. Walaupun wajah *web*nya bisa jadi sangat menyerupai atau sama, tapi kalau diminta registrasi ulang atau mengisi informasi sensitif, itu patut diwaspadai, misalnya halaman *login yahoo mail*. Disana akan disuruh memasukkan *username* dan *password e-mail* untuk *login*. Ketika mengklik tombol *login* maka informasi *username* dan *password* akan terkirim ke alamat pengirim *e-mail*. Jadi *e-mail* tersebut merupakan jebakan dari pengirim *e-mail* yang tujuannya untuk mendapatkan *password e-mail*.

Yang menjadi lebih runyam lagi, sekarang sudah ada beberapa *e-book* yang berkeliaran di internet untuk menawarkan teknik menjebol *password.* Seperti diketahui *password* merupakan serangkaian karakter, baik berupa huruf, *string*, angka, atau kombinasinya untuk melindungi dokumen-dokumen penting. Maka bisa dibayangkan jika *password e-mail* dijebol, yang terjadi adalah seluruh data-data akan dapat diketahui, termasuk *password Account Internet Banking* yang verifikasinya biasa masuk melalui *e-mail*.

Adapun hukum yang mengatur tentang *cybercrime* khususnya *cracker* dulunya masih bersifat umum dan

masih menggunakan Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP), Undang-Undang Telekomunikasi yang kemudian dilakukan interpretasi atau penafsiran terhadap undang-undang tersebut, sehingga suatu perbuatan yang tidak diatur dalam undang-undang tidak begitu saja dikesampingkan karena belum ada peraturan atau ketentuan yang mengaturnya. tetapi saat ini sudah ada undang-undang yang bersifat khusus yang mengatur tentang *cracker* yaitu UU ITE, khususnya terdapat dalam Pasal 30.

Dalam Pasal 30 UU ITE, Pasal ini merupakan kejahatan yang dilakukan oleh para *cracker* dengan modus operandi yang dapat dijelaskan sebagai berikut: *Pertama,* dilarang untuk: 1. Melakukan komunikasi, mengirimkan, memancarkan, atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau 2. Sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah. Kedua hal tersebut sebagaimana dijelaskan dalam penjelasan ayat 1 dan 2. Menurut pendapat penulis, dalam ayat 1 dan 2 ini seseorang dengan sengaja dan dengan suatu cara yang salah memasuki jaringan komputer orang lain tanpa izin guna memperoleh atau mencuri data milik orang lain tersebut merupakan perbuatan seorang *cracker* yang dilakukan dengan modus operandi dengan menerobos atau membobol pengamanan jaringan komputer milik orang lain untuk mendapatkan data-data yang diinginkan guna tercapainya perbuatan jahatnya.

Kedua, Dalam penjelasan Pasal 30 ayat 3: Sistem pengamanan adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer yaitu dengan berdasarkan suatu kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan. Menurut pendapat penulis, dalam ayat 3 ini disebutkan bahwa seseorang yang dengan sengaja mengakses komputer dan sistem elektronik dengan cara menerobos dan/atau menjebol sistem pengamanan yang dimiliki oleh pemilik atau *user* tersebut merupakan modus kejahatan dari seorang *cracker.* Para *cracker* melakukan hal tersebut guna memperoleh keuntungan bagi dirinya sendiri, yaitu baik dengan memperoleh keuntungan secara finansial yang menghasilkan uang banyak dengan menjebol *password* milik orang lain yang berhubungan dengan banking atau *credit card,* maupun *non financial* untuk memenuhi kepuasan dirinya sendiri dengan cara merusak jaringan komputer dan sejenisnya. Dengan diketahuinya *password* tersebut, maka dengan mudah *cracker* dapat melakukan kejahatannya.

Faktor-faktor yang Mempengaruhi Terjadinya *Cracker*

Di era kemajuan teknologi informasi ditandai dengan meningkatnya pengguna internet dalam setiap aspek kehidupan manusia. Meningkatnya pengguna internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan suatu aktivitasnya, di sisi lain memudahkan bagi pihak-pihak tertentu untuk dapat melakukan tindak pidana (Didik M. Arief Mansur dan Alisatris Gultom, 2006:95). Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya, lebih banyak di sebabkan oleh faktor keamanan si pelaku dalam melakukan kejahatan, dan masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal *cracker*. Berikut ini merupakan faktor-faktor yang mempengaruhi terjadinya *cracker*, antara lain adalah: Faktor politik; Faktor ekonomi; Faktor sosial budaya; Keresahan masyarakat pengguna komputer; dan Dampak *cracker* terhadap keamanan dalam negeri. Kelima hal tersebut akan dijelaskan satu per satu di bawah ini.

Faktor Politik

Dengan mencermati masalah *cracker* yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak, proses kriminalisasi di bidang *cracker* telah terjadi dan merugikan masyarakat. Media internet banyak memberitakan tentang *cracker* yang dilakukan oleh orang Indonesia, sebagaimana kasus yang terjadi di beberapa kota di Indonesia mengakibatkan citra Indonesia kurang baik di mata dunia dalam penegakan hukum *cracker*.

Serangan-serangan para *cracker* dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja maka dapat menimbulkan kekacauan pembayaran maupun transaksi keuangan bagi nasabah. Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi *cracker* yang berkembang di Indonesia. Untuk menghindari kerugian yang lebih besar akibat tindakan para *cracker* maka diperlukan suatu kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (*lex specialis*) bagi *cracker* yang saat ini telah diwujudkan dengan adanya UU ITE khususnya dalam Pasal 30.

Faktor Ekonomi

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi.

Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang memanfaatkan ini untuk mencari barang-barang kepentingan perorangan maupun korporasi. Produk barang yang dihasilkan di Indonesia sangat banyak dan sangat digemari komunitas internasional, seperti barang-barang kerajinan, ukiran, dan barang-barang lainnya. Para pelaku bisnis harus mampu dalam memanfaatkan sarana internet tersebut. Adapun krisis ekonomi yang telah melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk segera bangkit dari krisis tersebut. Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

Faktor Sosial Budaya

Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu: *Pertama,* kemajuan teknologi informasi. Pesatnya kemajuan teknologi informasi sungguh tidak dapat dibendung oleh siapapun di negeri ini. Semua orang membutuhkan teknologi, informasi, bahkan *levelitas* kebutuhan itu terhadap orang-orang tertentu yang maniak informasi dianggapnya sebagai sebuah kebutuhan primer, setelah kebutuhan makanan dan minuman. Sehari tanpa informasi, diibaratkan sehari tanpa minum, oleh karenanya tak mengherankan bahwa kemudian terbentuklah sebuah komunitas baru dunia Teknologi Informasi atau TI yang memainkan peran penting bagi kesejahteraan manusia, termasuk pertumbuhan ekonomi, politik, budaya, dan aspek kehidupan yang lain.

Pada era globalisasi ini, manusia tidak akan bisa melepaskan kebutuhannya atau teknologi informasi. Sehari-hari manusia bergantung dengan teknologi informasi, mulai dari yang sederhana sampai dengan yang super canggih. Yang sederhana seperti koran dan radio, namun keduanya ditunjang oleh teknologi yang canggih misalnya yang sehari-hari melekat pada tubuh manusia seperti *handphone* dan *laptop* untuk membantu aktivitasnya.

Dengan adanya teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena disitu ada kebebasan yang seimbang, bahkan dapat saja mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya. Menurut Agus Raharjo setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap suatu celah atau *bug* dalam memacu ekonomi dunia: Teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya; Dapat memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya (Agus Raharjo, 2002:1). Meskipun peranan tersebut lebih condong pada bidang ekonomi, namun dapat dilihat betapa pentingnya peranan teknologi informasi untuk dapat mengefektifkan layanan dan kepentingan sebagai tenaga dorong kemajuan komunikasi global dengan berbagai macam pihak agar maksud dan tujuan masing-masing dapat tercapai.

Kedua, adanya Sumber Daya Manusia (SDM) yang mengawali antara teknologi informasi dengan operator yang mengawaki mempunyai hubungan yang erat sekali, keduanya tak dapat dipisahkan. Sumber Daya Manusia dan teknologi informasi mempunyai peranan penting sebagai pengendali dari sebuah alat. Apakah alat itu digunakan sebagai alat kebajikan untuk mencapai kesejahteraan umat manusia, atau alat tersebut akan dikriminalisasikan sehingga dapat merusak kepentingan orang lain atau bahkan dapat merusak kepentingan negara dan masyarakat.

Teknologi informasi sebagai hasil temuan dan pengembangan manusia kemudian dimanfaatkan, untuk perbaikan-perbaikan umat, namun di sisi lain dapat membawa petaka bagi umat manusia sebagai akibat adanya penyimpangan. Di Indonesia sumber daya pengelolaan teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan suatu teknologi ini masih kurang. Penyebabnya ada berbagai hal, diantaranya kurang adanya tenaga peneliti dan kurangnya biaya penelitian atau mungkin kurangnya perhatian dan apresiasi terhadap penelitian. Sehingga sumber daya manusia di Indonesia lebih banyak sebagai pengguna saja dan jumlahnya cukup banyak.

Ketiga, komunitas baru. Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, diantaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuklah sebuah komunitas baru di dunia maya yakni komunitas para pecandu internet yang saling berkomunikasi, bertukar pikiran berdasarkan prinsip kebebasan dan keseimbangan di antara para pecandu atau maniak dunia maya tersebut.

Komunitas yang ada ini adalah sebuah populasi gaya baru sebagai gejala sosial, dan sangat strategis untuk diperhitungkan, sebab dari media ini, banyak hikmah yang bisa didapatkan. Dari suatu hal yang pada awalnya tidak tahu dapat menjadi tahu, dan suatu hal yang tahu jadi semakin pintar serta semakin canggih. Terjadinya perkembangan teknologi dan laju perkembangan masyarakat diketahui dengan cepat

dan akurat, dan mereka saling bertukar pikiran serta dapat melakukan *rechecking* di antara mereka sendiri.

Secara emosional, mereka melekatkan dirinya kepada teman sesama di dunia maya. Salah satu komunitas itu adalah adanya *mailing list.* Di *yahoo* terdapat komunitas dan kemudian difasilitasi oleh *yahoo* dalam bentuk *group.yahoo.com*. Dalam *mailing list* mereka dapat berdiskusi tentang suatu masalah, namun mereka tidak harus menghidupkan komputer dan internet secara bersamaan, sedangkan *chatting*, di antara mereka harus sama-sama menghidupkan komputer.

Keempat, dampak *cracker* terhadap keamanan negara. Setelah melihat dari beberapa faktor yang mempengaruhi terjadinya *cracker,* dampak *cracker* terhadap keamanan negara yaitu dapat disoroti dari beberapa aspek, antara lain: Kurangnya kepercayaan dunia terhadap Indonesia; Di sejumlah kota-kota besar yang ada seperti Bandung, Semarang, Yogyakarta, Surabaya, dan Jakarta, para *cracker* sebagian besar itu adalah dari oknum terdidik seperti mahasiswa. Kejahatan semacam ini terus berlangsung dalam beberapa tahun belakangan ini. Hukuman terhadap para *cracker* dulunya cukup ringan, bahkan banyak pihak berpendapat, pelakunya adalah pahlawan karena dapat membobol suatu situs dengan kemampuannya. Padahal, di balik kejahatan itu para pelaku telah menurunkan derajat dan martabat bangsa Indonesia di mata dunia, karena merugikan banyak pihak melalui teknologi informasi.

Kelima, dapat berpotensi menghancurkan negara. Perkembangan dari teknologi informasi yang ada membawa suatu dampak lain, yaitu tumbuh suburnya *cracker*, kejahatan melalui media internet. *Cracker* menjadi masalah serius yang harus segera ditangani. Kepolisian dan para penegak hukum lainnya harus peduli terhadap dampak yang ditimbulkan kejahatan ini dan berupaya serius untuk menanggulanginya. Tak ada satu negara pun di dunia ini yang terbebas dari ancaman *cracker*. Ini berkat kemampuan teknologi internet mengaburkan batas-batas fisik dan budaya sebuah negara.

Pencegahan terhadap tindak pidana *cracker*, harus mencakup semua operasi ilegal atau akses ke internet yang merugikan pihak lain. Operasi ilegal ini meliputi akses tanpa izin, merusak data atau program komputer, melakukan sabotase untuk menghilangkan sistem atau jaringan komputer, mengambil data dari dan kedalam jaringan komputer tanpa izin, serta memata-matai komputer.

Pelaku *cracking* bisa melakukan operasi ilegal itu disebabkan adanya jaringan komputer yang telah dimanfaatkan oleh semua pihak, baik pemerintah maupun pelaku ekonomi di Indonesia. Perbankan dalam memberikan pelayanan yang cepat terhadap pelanggan memanfaatkan jaringan komputer. Maka dapat diprediksikan akibatnya bahwa apabila ada serangan *cracker* baik sengaja atau hanya sekedar iseng melakukan penyusupan atau pengerusakan terhadap jaringan tersebut. Sektor perbankan akan lumpuh saat perangkat komputernya diganggu oleh *cracker*, hal ini bukan tidak mungkin dilakukan. Contohnya adalah yang terjadi pada jaringan KPU pada saat penghitungan suara. Data yang ada dapat diubah oleh pelaku. Kalau data perbankan diubah maka akan dapat menimbulkan masalah besar bagi nasabah yang jumlahnya sangat banyak. Kecanggihan teknologi ini menjadi semacam kegiatan *spionase* yang berpotensi menghancurkan negara.

Keresahan Masyarakat Pengguna Jaringan Komputer

Menurut TB. Ronny R. Nitibaskara, kejahatan atau *crime* tidak dapat dipisahkan dari lima faktor yang saling berhubungan, yaitu: pelaku kejahatan, modus operandi kejahatan, korban kejahatan, reaksi sosial atas kejahatan, dan hukum. Lebih jelasnya diuraikan sebagai berikut: 1. Pelaku kejahatan. Dalam hal pelaku kejahatan *cracker*, karakter subjek hukum berbeda dari pelakunya. Pelaku tampaknya memiliki keunikan tersendiri, yang belum tertampung dalam konsep-konsep atau teori konvensional mengenai tindak kejahatan; 2. Modus operandi kejahatan. Bahwa suatu modus operandi *cracker* sangat berbeda dari tindak kejahatan konvensional. yang paling mencolok dari perbedaan tersebut antara lain adalah *locus delicti* atau tempat kejahatan perkara karena sangat sulit melokalisir jaringan internet; 3. Korban kejahatan. Korban *cracker* tidak selalu dalam bentuk dapat dilihat atau *tangible* melainkan juga yang tidak terlihat atau *intangible* karena tempat tinggal dan kewarganegaraan korban yang tidak selalu sama dengan pelaku atau *cracker*, maka penegak hukum menghadapi masalah yang jauh lebih kompleks lagi; 4. Reaksi sosial atas kejahatan. Reaksi sosial atas suatu tindak kejahatan jauh lebih terukur ketimbang yang terjadi pada kasus *cracker*. Misalnya, reaksi massa terhadap perampok atau pencuri yang tertangkap berupa penghakiman massa. Sebaliknya, segmen masyarakat yang bereaksi atas suatu tindakan *cracker* tidak sebesar pada kasus konvensional. Namun demikian, dampak *cracker* tidak lebih kecil dibandingkan dengan kejahatan-kejahatan konvensional; 5. Hukum. Undang-undang dan perangkat hukum serta aturan lain yang bersifat

empirik hingga saat ini masih banyak diantaranya yang bersandar pada yurisprudensi. Sebaliknya, UU ITE baru disahkan pada bulan Nopember tahun 2008 dan perkembangan kerangka hukum yang ada kalah pesat dibandingkan dengan perkembangan kejahatan yang terjadi.

Dampak *Cracker* terhadap Keamanan Dalam Negeri

Ketidaksiapan Indonesia dalam mengantisipasi perkembangan teknologi informasi dalam bentuk struktur maupun infrastruktur hukum, bisa berakibat buruk dan bukan tidak mungkin ancamannya adalah kerawanan sosial dan politik yang ditimbulkan oleh individu-individu yang berperilaku menyimpang. Motif para *cracker* bukan hanya *money oriented*, tetapi juga melemparkan isu-isu yang meresahkan, memanipulasi simbol-simbol kenegaraan dan partai politik dengan tujuan untuk mengacaukan keadaan agar tidak tercipta suasana yang kondusif.

Selain ingin meraih keuntungan secara finansial dari kegiatan-kegiatan *cracker* tersebut, mereka juga berusaha merusak situs-situs perbankan, kartu kredit, toko-toko yang menawarkan barang secara *online*, lembaga-lembaga keuangan, bursa efek, kurs valuta asing, dengan maksud terjadinya kekacauan dalam bidang perdagangan.

PENUTUP

Kesimpulan

Setelah melakukan penelitian hukum terhadap bahan-bahan hukum yang membahas modus operandi *cracker* dan atas aktivitas *cracking* di internet, pada akhirnya diperoleh suatu simpulan: Modus operandi terhadap kejahatan-kejahatan para *cracker* disebut *Unauthorized Access to Computer System and Service,* yaitu melakukan suatu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Modus kriminalitas yang dilakukan *cracker*, salah satu bentuknya yang wajib diwaspadai adalah pencurian data-data *account* penting. Pelaku biasanya adalah seorang *cracker* dengan cara menjebak orang lain untuk tidak sadar bersedia memberikan data-data *account*-nya. Modus operandi *cracker* ini sangat berbeda dengan tindak kejahatan konvensional. Hal yang paling mencolok dari perbedaan tersebut antara lain adalah terletak pada *locus delicti* atau tempat kejahatan perkara karena dalam kejahatan ini yang diserang adalah jaringan komputer atau internet.

Rekomendasi

Modus kejahatan dalam dunia maya terutama kejahatan *cracker* memang agak sulit di mengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi. Sebab salah satu karakter pokok *cracker* adalah menggunakan teknologi informasi dalam modus operandinya. Terkait dengan korban *cracker*, maka yang pasti menjadi korbannya adalah suatu kalangan yang sama-sama menggunakan sarana teknologi informasi, khususnya internet. Untuk itu, bagi para pengguna teknologi informasi khususnya internet agar lebih hati-hati dan lebih meningkatkan pengamanan terhadap *software* maupun *hardware* jaringan komputer.

Dengan adanya UU ITE, maka diharapkan para penegak hukum agar lebih terampil, dan memiliki keterampilan dasar dalam menggunakan komputer dan internet serta lebih profesional dalam menangani kasus-kasus dunia maya, sehingga mampu mengatasi persoalan-persoalan hukum terutama terhadap *cracker* atas aktivitas *cracking*-nya di internet baik yang bersifat nasional, regional maupun internasional.

Dalam UU ITE agar lebih diperjelas lagi tentang pengaturan korporasi dan penjatuhan pidananya. Karena dalam undang-undang ini tidak memberikan penjelasan dengan tegas tentang makna korporasi itu sendiri, dan agar diatur pula tentang pengaturan pidana tambahan.

DAFTAR PUSTAKA

Buku:

Mansur, Didik M. Arief dan Elisatris Gultom, 2006, *CYBER LAW: Aspek Hukum Teknologi Informasi,* Jakarta: Refika Aditama.

Chasawi, Adhami, 2005, *Pelajaran Hukum Pidana 3*, Jakarta: Raja Grafindo Persada.

Hamzah, Andi, 2005, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta.

Huda, Chairul, 2006, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung-jawaban Pidana Tanpa Kesalahan*, Jakarta: Kencana.

Ibrahim, Johnny, 2006, *Teori dan Metodologi Penelitian Hukum Normatif,* Malang: Bayumedia.

Kohidin, M., *Cyber Crime, Modus Operandi dan Penanggulangannya*, Jogjakarta: LaksBang PRESSindo.

Kristanto, A., 2008, *Jadi Hacker Siapa Takut*, Yogyakarta: Universitas Atma Jaya Yogyakarta.

Manthovani, Reda, 2006, *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia,* Jakarta: Malibu.

Marzuki, Peter Mahmud, 2007, *Penelitian Hukum*, Jakarta: Kencana.

Moeljatno, 2000, *Asas-Asas Hukum Pidana,* Jakarta: Rineka Cipta.

Muladi, 2004, *Lembaga Pidana Bersyarat*, Bandung: Alumni.

Nawawi Arief, Barda, 2000, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, Semarang: Badan Penerbit UNDIP.

Purwoleksono, Didik Endro, 2008, *Diktat Hukum Pidana*, Surabaya: Fakultas Hukum UNAIR.

_____, 2008, *Makalah, Telaah Kritis Undang-Undang No. 11 Tahun 2008*, Surabaya: Fakultas Hukum UNAIR.

Ramli, Ahmad M., 2004, *CYBER LAW dan HaKI dalam Sistem Hukum Indonesia,* Bandung: Refika Aditama.

Riswandi, Budi Agus, 2006, *Hukum Cyberspace,* Yogyakarta: Gitanagari.

Ruslim, Harianto, 2006, *HACK ATTACK: Konsep, Penerapan dan Pencegahan,* Jakarta: Jasakom. Dapat dijumpai dalam situs internet: http://www.jasakom.com/penerbitan.

S'to, 2006, *Seni Internet Hacking Uncensored,* Jakarta: Jasakom. Dapat dijumpai dalam situs internet: http://www.jasakom.com/penerbitan.

Schaffmeister, et al., 2007, *Hukum Pidana*, Bandung: Citra Aditya Bakti.

Sholehuddin, 2004, *Sistem Saksi dalam Hukum Pidana*, Jakarta: Raja Grafindo Persada.

Sutarman, 2007, *CYBER CRIME: Modus Operandi dan Penanggulangannya,* Yogyakarta: LaksBang Pressindo.

Wahid, Abdul dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cybercrime),* Bandung: Refika Aditama.

Peraturan Perundang-undangan:

Kitab Undang-Undang Hukum Pidana

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Sumber Lain:

Detikinet, tt. *Hacker KPU divonis 6 bulan 21 hari*. Dapat dijumpai dalam situs internet: http://jkt1.detikinet.com/index.php/detik.read/tahun/2004/bulan/12/tgl/23/time/172827/idnews/261466/idkanal/110.

Detikinet. tt. *Pasal yang Dijeratkan pada Hacker Dinilai Lemah*. Dapat dijumpai dalam situs internet: http://www.detikinet.com/index.php/detik.read/tahun/2004/bulan/04/27/time/132554/idnews/129256/idkanal/110.

Koordinator ICT Watch, tt. *Cracker: Sebab Akibat dan Kepastian Hukum*. Dapat dijumpai dalam situs internet: http://free.vlsm.org/v17/com/ictwatch/paper/paper061.htm

My Personal Library Online. Tt.*Cyber crime*. Dapat dijumpai dalam situs internet: http://dhani.singcat.com/internet/modul.php.